Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

23 October 2017

PIN Number

171023-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@ic.fbi.gov

Phone:
1-855-292-3937

CrySiS Ransomware Targets US Businesses through Open RDP Ports

Summary

Between June 2016 and July 2017, CrySiS ransomware targeted hundreds of US businesses, to include churches, private businesses, medical facilities, law firms, and local governments vulnerable to Remote Desktop Protocol (RDP) implementations, CrySiS actors demanded cryptocurrency in exchange for a decryption key. The FBI assesses it is likely the cyber criminals used an open RDP port to deploy CrySiS ransomware. Using the RDP port for intrusion presents a challenge because the malware enters through an approved access point. This method decreases the likelihood of detection and ability for businesses to mitigate infection.

Threat

CrySiS actors appear to identify victims by scanning for open RDP ports. After gaining RDP access via dictionary attack, brute force attack, or using stolen login credentials, the actors escalate their privileges to administrator levels, drop the malware onto the server, and run an executable file, all without any action or knowledge on the part of the

victim. While many ransomware campaigns rely on a victim completing an action, such as opening an e-mail or visiting a compromised Web site, RDP allows cyber actors to infect victims with minimal detection.

Once infected and encrypted, CrySiS actors instruct victims to contact the actors' e-mail addresses for further instructions. These instructions are provided to victims through ransom notes left on desktops, as background images, or in folders on victim's computers. After establishing contact, the victim receives a ransom demand to be paid in the cryptocurrency Bitcoin (BTC) in exchange for a decryption key.

CrySiS actors do not change the name of files they encrypt, but they append their e-mail address and file extension to the existing file names. The file extensions associated with CrySiS ransomware are .crypt, .crysis, .dharma, .lock, .onion, .wallet, .xtbl, and .zzzzz. Private industry regularly develops decryption keys and tools for the CrySiS ransomware, causing CrySiS actors to develop newer versions, often with additional file extensions included.

In January 2017, the decryption keys for files encrypted with the .crypt, .crysis, .lock, and .xtbl file extensions were released publicly, likely by a CrySiS actor. Similarly, the decryption keys for .dharma were released in March 2017, and the decryption keys for .wallet were released in May 2017. As of September 2017, .onion decryption keys have not been released.

Cybersecurity companies likely will continue to develop decryption tools for variants including released decryption keys. However, the developers of CrySiS will likely continue to release new variants to infect victims and demand ransom payments as long as CrySiS actors are successful at infecting victims and victims continue to pay ransoms. A decrease or cessation of victim complaints and open source reporting on CrySiS infections would indicate CrySiS actors may be evolving their tactics, closing down the ransomware campaign, or having less success with infecting and/or profiting from victims.

Recommendations

The following list includes self-protection strategies against CrySiS ransomware campaigns:

- Avoid paying ransoms, as there is no guarantee information will be restored
- Back up data regularly
- Verify integrity of back up process
- Keep software updated
- Use strong passwords to protect RDP credentials
- If possible, use two factor authentication
- Audit who accesses RDP

- Establish whitelist access for RDP
- Consider disabling RDP if not in use
- Change RDP port from 3389 to another unused port
- Block RDP via firewall
- Audit logs for all remote connection protocols
- Audit logs to ensure all new accounts were intentionally created
- Scan for open or listening ports, and mediate

Administrative Note

This product is marked **TLP:GREEN**. Recipients may share **TLP:GREEN** information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. **TLP: GREEN** information may not be released outside of the community.

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey